UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

BRAINCHILD SURGICAL DEVICES, LLC, *Plaintiff*, vs. CPA GLOBAL LIMITED, *Defendant*.	Civil Action No. 1:21-cv-00554-RDA-JFA

MEMORANDUM OF LAW OPPOSITION TO DEFENDANT'S MOTION TO COMPEL

CPA Global Limited ("CPA" or "Defendant") seeks to compel documents from Maimonides Medical Center, the former employer of the class representative Dr. Sherwinter for the plaintiff Brainchild Surgical Devices ("Brainchild" or "Plaintiff") for information stored on their servers that contain attorney-client communications between Dr. Sherwinter and Brainchild's counsel. The question presented is simply whether using an email ultimately stored on an employer's server waives the attorney-client privilege. While the Defendant points to Virginia law, the balancing test applied has been largely standardized across the federal courts, which provide more specific guidance. Surveying the case law, as long as there is a reasonable expectation of privacy, the mere fact that an employer *can* access attorney-client communications does *not* waive the privilege.

In this case, Dr. Sherwinter had a clear understanding with his employer that he could trust the privacy of his communications using his work email, and therefore, he had a reasonable

expectation of privacy that justifies maintaining the attorney-client privilege. As such, the objection to the production of such privileged materials should stand, and the Defendant's motion to compel should not be granted.

I. BACKGROUND AND PROCEDURAL HISTORY

Dr. Sherwinter is an inventor who made use of CPA's services on side-projects he was working on while at Maimonides. Declaration of Dr. Daniel Sherwinter ("Sherwinter Decl."), ¶¶ 2, 3. From 2006 until 2022, Dr. Sherwinter was allowed to use his computer and email for personal and Brainchild purposes. *Id*. Nobody at Maimonides questioned or had any issue with it, and he kept his information private using a password. Additionally, his computer was located in a locked office. *Id*. All of Dr. Sherwinter's conversations with his supervisors and IT and HR staff led him to believe that his email was fully private and secure, notwithstanding if he committed illegal activities, which he never did. Sherwinter Decl. at ¶ 4. As he never engaged in illegal activities, he never believed he would lose any privacy. *Id*.

Afterward, as described in Defendant's motion, Maimonides, who maintains the server, was subpoenaed for Dr. Sherwinter's communications. Brainchild raised its objections and raised attorney-client privilege in a timely manner. Declaration of Ryan Abbott ("Abbott Decl."), ¶ 3. As an additional protection, CPA's counsel agreed that Maimonides could produce documents directly to Brainchild's counsel instead of CPA to allow for further protection of privileged materials. Abbott Decl. ¶ 3. Counsel for Brainchild duly reviewed all documents provided by Maimonides, withheld various documents based on attorney-client privilege as noted in a privilege log provided to CPA Global, and produced the balance of documents directly to CPA Global. Abbott Decl. ¶ 4. Counsel for CPA Global agreed to the above process, but noted they were not waiving any arguments with respect to privilege. Abbott Decl. ¶ 5.

II. ARGUMENT

In *Banks v. Mario Industries of Virginia, Inc.*, 274 Va. 438 (2007), the Virginia Supreme Court stated that because "Mario's employee handbook provided that there was no expectation of privacy regarding Mario's computers" this constituted a waiver of the attorney-client privilege for documents created and saved on work computers. *Banks v. Mario Indus. of Virginia, Inc.*, 274 Va. 438, 454 (2007). But this is not an absolute rule. The question is what constitutes an adequate expectation of privacy so as not to waive attorney-client privilege, given the requirement that such communications be made in confidence. *See id*. The Court did not evaluate the handbook in *Mario Industries,* but most federal courts have applied a similar analysis when looking at similar sets of facts, which clarifies what it means to not have an expectation of privacy on a work computer.

The federal courts have consistently ruled that employees can maintain privilege for communications made with their attorneys on work computers using work emails. The case law shows that "question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable." *Sprenger v. Rector & Bd. of Visitors of Virginia Tech*, No. CIV.A. 7:07CV502, 2008 WL 2465236, at *3 (W.D. Va. June 17, 2008). "Accordingly, the objective reasonableness of that intent will depend on the company's e-mail policies regarding use and monitoring, its access to the e-mail system, and the notice provided to the employees." *Hanson v. First Nat. Bank*, No. CIV.A. 5:10-0906, 2011 WL 5201430, at *5–6 (S.D.W. Va. Oct. 31, 2011). Another potentially "deciding factor: with respect to privilege issues" is "how did [the employer] interpret its computer usage policy." *United States v. Hatfield*, No. 06-CR-0550 (JS), 2009 WL 3806300, at *10 (E.D.N.Y. Nov. 13, 2009).

A sister court in West Virginia recently found even more starkly that a company policy

cannot undermine such a "sacrosanct" privilege unilaterally: "That Under Armour would purport to invade such a sacrosanct privilege, by operation of its unilateral IT policies, is, in a word, offensive. Just because Under Armour decrees to its employees (who presumably have no say in the matter) that they give up virtually all expectation of privacy should not necessarily make it so. Certainly, it is understandable that Under Armour might impose some sort of IT usage policy to safeguard its business operations, infrastructure, productivity, and privacy. But it is beyond the pale, as the undersigned concluded before, that an employer could purport to override certain fundamental legal privileges of its employees." *Pajak v. Under Armour, Inc.*, No. 1:19-CV-160, 2021 WL 2154857, at *3 (N.D.W. Va. May 26, 2021).

The case law, and even the legal analysis from the Defendant, ultimately leads to the conclusion that the question is whether Dr. Sherwinter was told he should have no expectation of privacy. Unlike the cases Defendant relies on, there is more to Dr. Sherwinter's expectations than an employee handbook, as he was also given assurances over the 16 years he worked at Maimonides that his personal use of email and his computer was fine, and that he had privacy. *See* Sherwinter Decl. ¶¶ 2-4. The policy Defendant relies on is also written in a way that does not clearly or directly contradict the course of conduct and verbal representations that Maimonides made to Dr. Sherwinter. Looking closely at the policies, in fact, Maimonides communicated that it respected private matters.

The policies at issue in this case do not prohibit any actions taken by Dr. Sherwinter. First, "Personal use of e-mail and electronic messaging is permitted on a limited basis." (Maimonides Medical Center Electronic Mail Policy, contained in Exhibit 7 to the Motion, ("Policy") at 1). Although there is a header that states "no assurance of privacy," the specific language of the agreement shows that, in fact, there are assurances of privacy for users. See Policy at 2. The

reason there is "no guarantee" of privacy is purely because of either legal processes, like subpoenas, or similar investigations of misconduct. (Policy at 2). The policy states that "Since courts have required Communications sent, received and/or stored via company e-mail and electronic messaging services to be disclosed in response to legal process (i.e., discovery, subpoenas) or to law enforcement officials, Users understand that the Medical Center cannot guarantee the privacy of Communications sent, received and/or stored using e-mail and electronic messaging services provided by the Medical Center." It also does not guarantee privacy for "behavior prohibited by the law or Medical Center policies, and/or as otherwise necessary for legitimate business purposes." The gist is that the Policy warns against the privacy of information per a legal process, but Gmail or other non-work emails would have the same limitations if faced with a court order. So, that cannot mean that there was no reasonable expectation of privacy, or Plaintiff would be able to obtain any email ever drafted between Defendant and its counsel as well from their use of insecure electronic communications.

The handbook discusses email security in general terms, and thus recommends securing it to obtain privacy. "E-mail and electronic messaging is not a secure means of communication." *Id*. Thus, the users were "required to protect the confidentiality of their log-on usernames and passwords and must not share such codes with others. Users should take precautions against others obtaining access to their email or electronic messaging." *Id*. at 4. Thus, instead of warning that workers cannot expect privacy from the company, it is a general warning about electronic communications and the need to protect privacy. It would be an absurd result to see a company tell an employee to protect their privacy, and then find they had no expectation of the same privacy. Alternatively, if this is read to warn against email as an insecure method of communication, it would once again support a finding that no email communications between an

attorney and client would ever be protected, which would be an absurd result.

Applying the factors from *In re Asia Global Crossing, Ltd.,* 322 B.R. 247, 257 (Bankr. S.D.N.Y.2005), as CPA advocates for, it shows that Dr. Sherwinter had an objectively reasonable expectation of privacy. The factors are "(1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies." *Id*.

Unequivocally, Maimonides allowed personal use, as it specifically says "[p]ersonal use of e-mail and electronic messaging is permitted on a limited basis." (Policy at 1.) This is reiterated on the third page, where it states that "excessive sending and/or receiving e-mail or electronic messaging for non-business purposes" is disallowed. What this limit appears to be is "personal use may be restricted if the resources consumed interfere with utilization of the computer system for business purpose." (Policy at 1.) To the extent specific uses were banned, these were illegal acts. *See* Policy at 2 (The section entitled "no assurance of privacy" regards specifically, "response to legal process or government or law enforcement" despite some more general language, creating a clear impression of illegal or similar activity being the trigger for any loss of privacy.) This is essentially stating a truism because that would be the case no matter the policy. In effect, personal use was allowed with no real restriction, which was made even more clear to Dr. Sherwinter after 16 years of consistently allowing him full privacy and freedom to use his email for personal matters, including matters related to Brainchild.

Unlike the case law cited by the Defendant, the policy itself is not the sole basis for understanding the impression created in the workplace. Dr. Sherwinter worked at Maimonides for

16 years, and during this time, he was assured and repeatedly was given the impression by everyone that he had a password protected, private and secure email system. Sherwinter Decl. ¶¶ 2-4. Likewise, he was given the impression that he was entirely allowed to use his email for business matters for Brainchild, and the persons making the privacy policy knew about this and never admonished or warned him against it. *Id*. In conjunction with the manner in which the policy is drafted, it creates a clear impression that any reasonable person would believe does not include emails of the nature Defendant is seeking.

As to the second factor, the company's monitoring policy is largely restricted to "responses to legal processes and law enforcement officials." Policy at 4. This monitoring is "as necessary." *Id.* While this may appear broad on its face, in practice, it relates to, as the Policy states, "suspected policy violations" after security is "notified." *Id*. The overall tenor of the rule is that law breaking will be checked, as in actual security breaches instead of private legal communications. This was the understanding that Dr. Sherwinter had. Not only did he understand that personal use was fine, he understood that only illegal activity would be checked, and he would be notified in the event this occurred. Sherwinter Decl. at ¶ 3. At no time in 16 years at the company was Dr. Sherwinter ever informed that his email was being checked and given that he never committed a crime in the use of his email, he believed he had full privacy. *Id*. This fit the overall course of conduct and discussions around the procedure and policy, and it is logical given the examples given in the Policy.

Likewise, the right of third parties to access the email was apparently limited to security violations. Policy at 4. This was what was actually communicated to Dr. Sherwinter, and it comports with the overall thrust of the Policy. Given that this was the level of communication provided, and it ultimately gave a sense of security to Dr. Sherwinter, it would be inequitable to

find a waiver of privilege when he was led to believe he had secure email. Sherwinter Decl. at ¶ 3.

The Fifth Circuit's analysis of a similar situation where there was some degree of access, but an expectation of privacy as to most people the majority of the time and found that this creates a meaningful expectation of privacy. *See United States v. Slanina*, 283 F.3d 670, 676–77 (5th Cir.), *cert. granted, judgment vacated on other grounds*, 537 U.S. 802 (2002).[1] The Court first found that "Slanina did exhibit a subjective expectation of privacy, we now must decide whether this expectation was objectively reasonable." *Id*. The government argued numerous factors militated against a reasonable expectation of privacy. It argued that "other city employees had a grand master key to Slanina's office . . . the city's need to develop network systems and upgrade equipment required complete computer access, and that Slanina's installation of the passwords did not change this situation. Finally, it points out that the computer was purchased by the city and that employees knew they were not allowed to use city computers to access and store pornography. Given these circumstances, the government contends, any expectation of privacy was unreasonable. We disagree." *Id*.

The Court found that these factors were undercut on the totality of the circumstances. For instance, "Slanina had a private office at the new fire station, and the ability of a select few of his coworkers to access the office does not mean that the office was 'so open to fellow employees or the public that no expectation of privacy is reasonable.' *Id*. (Quoting *O'Connor v. Ortega,* 480 U.S. 709, 718 (1987).) In addition, access alone was not critical, rather whether it was routine was

[1] The reversal did not have to do with any of the findings on privacy, and these findings were explicitly upheld in the Fifth Circuit, explaining that its findings as to privilege remained law of the case, stating that, "Slanina concedes that the issue is foreclosed because it was raised and decided in his original direct appeal, but states that he is raising it to preserve it for possible Supreme Court review . . . this court will not reexamine this issue." *United States v. Slanina*, 359 F.3d 356, 358 (5th Cir. 2004).

what would militate against an expectation of privacy. *See id*. ("[E]ven though network administrators and computer technicians necessarily had some access to his computer, there is no evidence that such access was routine.") (Citing *Leventhal v. Knapek,* 266 F.3d 64, 74 (2d Cir. 2001) (finding that a government employee's expectation of privacy was reasonable and noting that state agency's access to computers did not appear to be frequent, widespread, or extensive). In addition, "the city did not disseminate any policy that prevented the storage of personal information on city computers and also did not inform its employees that computer usage and internet access would be monitored." *Id*. Thus, "given the absence of a city policy placing Slanina on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer, we hold that Slanina's expectation of privacy was reasonable." *Id*.

Applying the same standard to the totality of the circumstances, Dr. Sherwinter also had a reasonable expectation of privacy. There was no frequent monitoring, nor a warning of frequent monitoring from his employer. *See* Policy at 1-5. He also never experienced any monitoring or question as to his use over the course of his entire time at Maimonides, frequently using his email for personal purposes over the sixteen-year period he worked at the company. Sherwinter Decl. at ¶ 4. As in *Slanina*, review of his computer and/or emails either never happened or was extremely rare; nobody had routine access to his computer. *Id*. Dr. Sherwinter also had a private office, and password protected his computer. *Id*. Given the company's actual practice and the thrust of the Policy, Dr. Sherwinter's belief that he had privacy was reasonable.

If it is unclear if the privilege was waived, the Court should err on the side of preservation and protecting the attorney-client privilege. Refusing to protect the communications Dr. Sherwinter made with his attorneys under these facts would have dire consequences. The attorney-

client privilege is the oldest common law privilege. *Upjohn Co. v. U.S.*, 449 U.S. 383, 389 (1981). Courts have long recognized that the purpose of the privilege is to "encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice." *Id.* Sound legal advice and advocacy serve public ends, and "such advice or advocacy depends upon the lawyer's being fully informed by the client." *Id.* Therefore, waiver of the attorney-client privilege "is not lightly presumed." *U.S. v. Kendrick*, 311 F.2d 110, 116 (4th Cir. 1964).

In this Circuit, Judge Niemeyer wrote "[b]ecause a waiver of the attorney -client privilege—one of the most important and protected in the law—should be clear, I agree that we should not, in such an ambiguous circumstance, default to find a waiver." *In re Grand Jury* 16-3817 (16-4), 740 F. App'x 243, 249 (4th Cir. 2018) (Niemeyer, J. Concurring.) "[T]he attorney -client privilege serves an important purpose, and waiver should not be lightly presumed." *SD3, LLC v. Black & Decker (U.S.), Inc.*, No. 114CV00191CMHIDD, 2016 WL 4722001, at *5 (E.D. Va. July 29, 2016), aff'd in part, rev'd in part, No. 1:14-CV-00191, 2016 WL 11784677 (E.D. Va. Sept. 12, 2016). The privilege is so important that even when courts find that a party has waived objections, they often find an exception for objections based on the attorney-client privilege. *See, e.g., Zornes v. Specialty Indus., Inc.,* 166 F.3d 1212 at *3 (4th Cir. 1998) (The magistrate judge "ordered Appellants to submit completely their responses without objections, with the exception of objections based upon attorney work-product or attorney-client privilege."); *Primrose v. Castle Branch, Inc.*, 2016 WL 917318 (E.D.N.C. Mar. 8, 2016) (ordering that a plaintiff providing late discovery responses could only assert objections as to claims of attorney-client privilege and work product protection).

Finally, Defendant's argument that there was a waiver caused by Maimonides reviewing

the files when responding to the subpoena puts the cart before the horse. In any circumstance, someone will maintain an email server. In such circumstances, if the person who maintains the email server is a third party as is most often the case someone aside from the parties communicating with their attorneys will have the ability and legal duty to review documents under its control when faced with a subpoena. This means that in any circumstance involving electronic communications, if the party to the action responding to discovery isn't Google, Yahoo, etc., there will be a third party who is legally bound to review documents to respond to a subpoena that can include privileged material. The exception that Defendant advocates for would therefore subsume the rule.

In this exact context, the Eastern District of New York "notes that a general rule holding that individuals waive privilege by storing personal documents on a company computer could have significant unintended but very damaging consequences . . . Creating a broad waiver rule would not only impose a severe legal prejudice for nothing more than a (possible) violation of a company's internal policy, it could also subject companies to third party subpoenas seeking 'waived' privileged documents." *United States v. Hatfield*, No. 06-CR-0550 (JS), 2009 WL 3806300, at *10 (E.D.N.Y. Nov. 13, 2009). A broad waiver, however, is exactly what Defendant is asking for with its argument that privilege, if it ever existed, was waived.

Defendant advocates that even in a circumstance where Dr. Sherwinter reasonably believed he would have privacy; CPA should be entitled to communications with his attorney. It would be a grossly disproportionate and harsh to punish the Plaintiff and reveal privileged communications based on a reasonable belief of privacy after 16 years of consistent communications and expectations supporting his course of conduct.

Logically, given the existence of privilege for third-party stored communication in at least

some instances, it cannot be the case that because the party maintaining the email server accesses protected communications as part of its overall review for document production, it automatically waives the attorney-client privilege. If it were the case, there would be no test or analysis necessary to obtain attorney-client communications. Notably, CPA never suggests how Defendant could have taken precautions to eliminate privileged materials from a third party's server, because it is impossible. Instead, as described in counsel's declaration, Brainchild performed a privilege review after receiving the documents from Maimonides, which was the only practical way to preserve privilege. Abbott Decl. ¶ 3-5, Exs. A-C. There simply would never be privilege, because there is no way for a party to prevent the review of documents in the third party's possession, they can only object to their production which Brainchild did in this case. Abbott Decl. ¶ 3.

Given that the courts are very clear that privilege *can* exist even if one maintains emails on a server accessible by a third party, the rule cannot be what Defendants argue, as it avoids the analysis altogether. Ultimately, the test should be applied, and in this case, it maintains privilege. Thus, to the extent that there was any review by Maimonides that identified the existence of attorney-client privileged materials, Plaintiff maintains that they are privileged, and they should not be produced. Maimonides complied with Plaintiff's objection and quarantined the materials. This is the reason why Defendant has filed the motion to compel. So, it is erroneous on the facts, on their face, to say that there was waiver, and to find waiver would subsume the rule and undercut the settled law and balancing test to be applied. As applied, the privilege should be preserved and the Defendant's motion should be denied.

III. CONCLUSION

Brainchild respectfully requests that the Court deny the Defendant's motion in its entirety.

Respectfully submitted,

Dated: July 26, 2023

BROWN NERI SMITH & KHAN, LLP

By: /s/ Geoffrey A. Neri

Geoffrey A. Neri, Esq. VSB No. 72219
Ethan J. Brown, Esq. (pro hac vice)
Ryan B. Abbott, MD, PhD, Esq. (pro hac vice)
11601 Wilshire Blvd., Ste. 2080
Los Angeles, CA 90025
Phone: (310) 593-9890
Fax: (310) 593-9980
Geoff@bnsklaw.com
Ethan@bnsklaw.com
Ryan@bnskaw.com

Attorney for Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on Wednesday, July 26, 2023, I filed the foregoing document electronically with the Clerk of the Court using the ECF system, and caused to be served by electronic mail a copy of the foregoing document upon the following parties:

QUINN EMANUEL URQUHART & SULLIVAN, LLP
Eric C. Lyttle, VSB No. 48518
Jared W. Newton, VSB No. 80746
Meghan M. McCaffrey (pro hac vice)
J. Matthew Hamann (pro hac vice)
Michael L. Fazio (pro hac vice)
Anthony P. Alden (pro hac vice)
1300 I Street, NW, Suite 900
Washington, D.C. 20005
Phone: (202) 538-8000
Fax: (202) 538-8100
ericlyttle@quinnemanuel.com
jarednewton@quinnemanuel.com
meghanmccaffrey@quinnemanuel.com
matthewhamann@quinnemanuel.com
michaelfazio@quinnemanuel.com
anthonyalden@quinnemanuel.com

Counsel for Defendant

Dated: July 26, 2023

BROWN NERI SMITH & KHAN, LLP

By: /s/ Geoffrey A. Neri

Geoffrey A. Neri, Esq. VSB No. 72219
Ethan J. Brown, Esq. (pro hac vice)
Ryan B. Abbott, MD, PhD, Esq. (pro hac vice)
11601 Wilshire Blvd., Ste. 2080
Los Angeles, CA 90025
Phone: (310) 593-9890
Fax: (310) 593-9980
Geoff@bnsklaw.com
Ethan@bnsklaw.com
Ryan@bnskaw.com

Attorney for Plaintiff and the Proposed Class